

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-014441

(43)Date of publication of application : 19.01.2001

(51)Int.Cl.

G06K 19/073

G06F 12/14

G06K 17/00

H04L 9/32

(21)Application number : 11-374788

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.12.1999

(72)Inventor : HIROTA TERUTO  
TATEBAYASHI MAKOTO  
YUGAWA YASUHEI  
MINAMI MASANAO  
KOZUKA MASAYUKI

(30)Priority

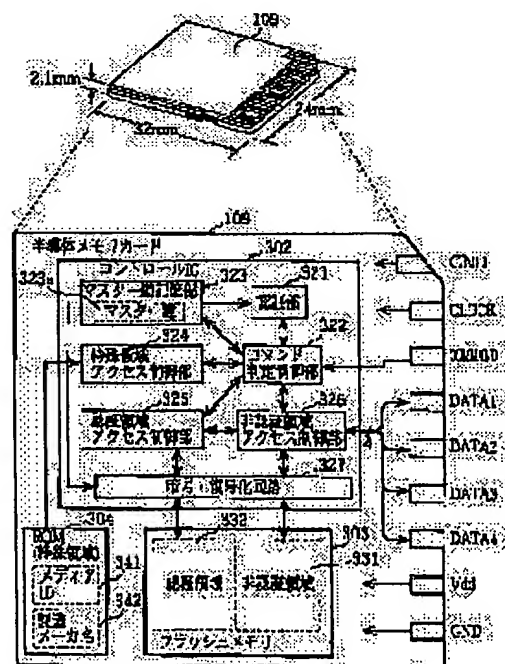
Priority number : 11119441 Priority date : 27.04.1999 Priority country : JP

## (54) SEMICONDUCTOR MEMORY CARD AND READER

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a semiconductor memory card usable as a storage medium for digital literary works and also usable as a storage medium for general computer data (non-literary works) for which the protection of copyright is not required.

**SOLUTION:** This card is composed of a control IC 302, a flash memory 303 and a ROM 304, the ROM 304 holds a medium ID 341 or the like peculiar to this card, the flash memory 303 has an authentication area 332 for permitting access to external equipment only when the authentication of that external equipment is made successful and a non-authentication area 331 for permitting access regardless of the authenticated result and the control IC 302 has control parts 325 and 326 for controlling access from the external equipment to the authentication area 332 and the non-authentication area 331 and an authentication part 321 or the like for executing mutual authentication with the external equipment.



Best Available Copy

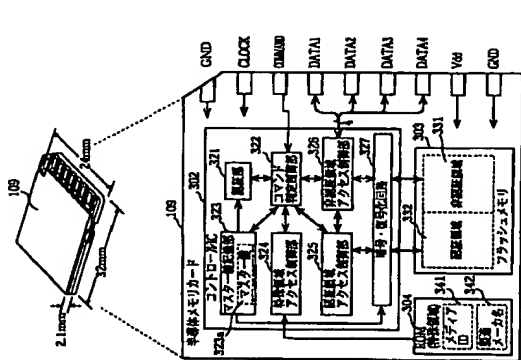
特開 2001-14441  
(P 2001-14441A)  
(43) 公開日 平成13年1月19日(2001.1.19)

| (51) Int. Cl. <sup>7</sup> | 種別記号                    | F I          | チャート <sup>1</sup> (参考)       |
|----------------------------|-------------------------|--------------|------------------------------|
| G 06 K 19/073              |                         | G 06 K 19/00 | P 58017                      |
| G 06 F 12/14               | 3 2 0                   | G 06 F 12/14 | 3 2 0 A 58035                |
| G 06 K 17/00               |                         | G 06 K 17/00 | E 58058                      |
| H 04 L 9/32                |                         | H 04 L 9/00  | 6 7 5 A 51104                |
|                            |                         |              | 6 7 5 D                      |
| 審査請求 未請求                   | 請求項の数 17                | OL           | (全 27 頁)                     |
| (21) 出願番号                  | 特願平11-374788            | (71) 出願人     | 00005821<br>松下電路産業株式会社       |
| (22) 出願日                   | 平成11年12月28日(1999.12.28) | (72) 発明者     | 松田 照人<br>大阪府門真市大字門真1006番地    |
| (31) 優先権主張番号               | 特願平11-119441            | (72) 発明者     | 阪本 誠<br>大阪府門真市大字門真1006番地     |
| (32) 優先日                   | 平成11年4月27日(1999.4.27)   | (74) 代理人     | 100090446<br>弁理士 中島 司朗 (外1名) |
| (33) 優先権主張国                | 日本 (J P)                |              |                              |

(54) 【発明の名称】 半導体メモリカード及び読み出し装置

(57) 【要約】

【課題】 デジタル著作物の配信媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の配信媒体としても用いることが可能な半導体メモリカードを提供する。  
【解決手段】 コントロールIC302とフラッシュメモリ303とROM304とからなり、ROM304は、このカードに固有のメディアID341等を保持し、フラッシュメモリ303は、外部機器の認証に成功した場合のみその外部機器に内蔵されたアクセスを許可する領域332と認証の結果にアクセスを許可する領域333とを有し、コントロールIC302は、外部機器による認証領域332及び非認証領域3331へのアクセスを制御する制御部325、326及び外部機器との相互認証を実行する認証部321等を有する。



と物理アドレスとの対応を示す変換テーブルと、前記電子機器からの命令に従って前記変換テーブルを更新する変換テーブル変更部とを有し、前記変換テーブルの変更部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御することを特徴とする請求項1記載の半導体メモリカード。

【請求項13】 前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項14】 前記不揮発メモリは、フラッシュメモリであり、

前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記非認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リストを読み出し部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項15】 前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であることをユーザに要求するものであり、

前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、

前記認証部による認証に成功した電子機器を特定することができるとして、前記ユーザキー記憶部に記憶されているユーザキーを参照し、既に格納されている場合に、前記認証部によるユーザキーの要求を察し、ユーザキー要求禁止部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項16】 請求項1記載の半導体メモリカードに格納されたデジタル著作物を読み出す装置であって、

前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、

前記読み出し装置は、

前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているかを判断する判断手段と、

許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする読み出し装置。

【請求項17】 請求項1記載の半導体メモリカードに

格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、

前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、前記読み出し装置、

前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、

10 前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているかを判断する判断手段と、

許可されている場合にのみ前記デジタル著作物をデジタル信号のままで外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする読み出し装置。

【発明の詳細な説明】

【0001】 本発明は、デジタル著作物を記憶するための半導体メモリカード及びその読み出し装置に関する。特に、デジタル著作物の著作権保護に好適な半導体メモリカード及び読み出し装置に関する。

【0002】 従来技術 近年、マルチメディア・ネットワーク技術の発展により、音楽コンテンツ等のデジタル著作物のインターネット等の通信ネットワークを通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。例えば、パーソナルコンピュータ（以下、「PC」という。）で音楽コンテンツをダウンロードした後、PCに格納された半導体メモリカードに格納しておくことで、必要に応じて音楽を再生し楽しむことができる。また、このようにして音楽コンテンツを格納した半導体メモリカードをPCから取り出して携帯型音楽再生装置に装着しておくことで、歩きながら音楽を聴くこともできる。このような半導体メモリカードは、フラッシュメモリ等の不揮発性で、かつ、大きな記憶容量の半導体メモリを内蔵した小型容量の便利なカードである。

【0003】 ここで、このような電子音楽配信において、半導体メモリカードにデジタル著作物を記憶する場

合、不正なコピーを防止するために、鍵等を用いてコンテンツを暗号化しておく必要がある。また、PC等に照準照付されて広く出回っているファイル管理ソフトウェアによって他の記憶媒体等にコピーすることができないようにしておく必要がある。

【0004】 このような不正なコピーを防止する方法として、半導体メモリカードへのアクセスを専用のソフトウェアでのみ可能とする方法が考えられる。例えば、PCと半導体メモリカード間での認証が成功した時のみ

半導体メモリカードへのアクセスを許可することとし、

専用のソフトウェアがないためにその認証に成功することができない場合には半導体メモリカードへのアクセスが禁止されるとする方法が考えられる。

【0005】

【発明が解決しようとする課題】 しかしながら、PCが半導体メモリカードにアクセスするのには専用のソフトウェアが必要とされるのではなく、そのような専用のソフトウェアを所有していない不特定多数のユーザと半導体メモリカードを介して自由にデータ交換し合うことが不可能となってしまう。そのために、フラッシュATAやコンパクトフラッシュ等の従来の半導体メモリカードが有していた利便性、即ち、専用のソフトウェアを必要とすることなくPCに標準添付されているファイル管理ソフトウェアでアクセスすることができるといった利便性が得られなくなってしまう。

【0006】 つまみ、専用のソフトウェアのみでアクセス可能な半導体メモリカードは、著作権保護の機能を有する点でデジタル著作物の記憶媒体としては適しているが、汎用的な使用が困難であるために一般的なコンテンツターミナルシステムにおける補助記憶装置として使用することができないという問題点がある。そこで、本発明は、この

ような問題点に鑑みられたものであり、デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカード及びその読み出し装置を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記目的を達成するためには、本発明に係る半導体メモリカードは、電子機器に装着可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた2つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御部とを備え、前記制御部は、前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証部を備える認証部と、前記認証部が認証に成功した場合にだけ前記非認証領域への前記電子機器によるアクセスを許可する非認証領域アクセス制御部とを有することを特徴とする。

【0008】 ここで、前記半導体メモリカードはさらに、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備えてもよい。また、本発明に係る読み出し装置は、上記半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数

が格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているかを判断する判断手段と、許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする。

【0009】

【発明の実施の形態】 以下、本発明の実施の形態について、図面を用いて説明する。図1は、通信ネットワークを介して音楽コンテンツ等のデジタル著作物をダウンロードするPCと、そのPCに接続可能な半導体メモリカード（以下、単に「メモリカード」という。）の外観を示す図である。

【0010】 PC102は、ディスプレイ103、キーボード104及びスピーカ106等を備え、内蔵するメモリ101によって通信回路101に接続されている。そして、このPC102が有するPCMCIAS等のカードスロット（メモリカード挿入口105）には、メモリカード107が挿入されている。メモリカード107は、PC102とメモリカード109を電気的に接続するアダプタであり、そのメモリカード109は、メモリカード109が装着されている。このメモリカード109は、以下の手順を踏むことで、インターネットにあるコンテンツプロバイダが提供する音楽データを取得することができる。まず、ユーザは、所望の音楽コンテンツを、通信回路101を通じて、PC102内のハードディスクにダウンロードする。音楽データは暗号化されており、そのままではPC102では再生することはできない。

【0012】 再生するためには、ダウンロード元のコンテンツプロバイダへクレジットカード等を用いてお金を払う必要がある。支払いを済ますと、コンテンツプロバイダよりパスワードと権利情報入手することができ、パスワードは、暗号化された音楽データを解除するために必要な鍵データである。権利情報は、PCでの再生可能回数や、メモリカードへの書き込み可能回数、再生可能な期間を示す再生制限等のユーザに許可された再生条件を示す情報である。

【0013】 パスワードと権利情報を取得したユーザは、PC102のスピーカ106から音楽を再生出力させる場合には、著作権保護機能が付いた専用のアプリケーションプログラム（以下、このプログラムを単に「アプリケーション」という。）に対して、入手したパスワードをキーボード104から入力する。すると、そのアプリケーションは、権利情報を検証した後に、暗号化された音楽データをパスワードを用いて復号しながらスピーカ106を通じて音声として再生出力する。

【0014】 また、権利情報としてメモリカードへの書き込み

き込みが許可されている場合には、そのアプリケーションは、時系列化された音楽データ、パスワード、権利情報はメモリカード109に書き込むことができる。図2は、このメモリカード109を記録媒体とする携帯型の録音再生装置（以下、「プレーヤ」という。）201の外観を示す図である。

【0015】プレーヤ201の上面には、液晶表示部203と操作ボタン202が設けられ、手前側には、メモリカード109を挿脱するためのメモリカード挿入口206及びPC102等と接続するためのUSB等の通信ポート213が設けられ、右側面には、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223等が設けられている。

【0016】プレーヤ201は、メモリカード109に格納された音楽データ、パスワード、権利情報に基づいて、再生が許可されている状態にあるならば、その音楽データを読み出して復号した後にアナログ信号に変換し、アナログ出力端子204に接続されたヘッドフォン208を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力端子205に出力したりする。

【0017】また、このプレーヤ201は、マイク等を介してアナログ入力端子223から入力されるアナログの音声信号をデジタルデータに変換してメモリカード109に記録したり、通信ポート213を介して接続されたPC102と通信することによって、そのPC102によってダウンロードされた音楽データ、パスワード及び権利情報をメモリカード109に記録することができ、つまり、このプレーヤ201は、メモリカード109への音楽データの記録及びメモリカード109に記録された音楽データの再生に関して、図1に示されたPC102及びメモリカード107に置き換わる機能性を有する。

【0018】図3は、PC102のハードウェア構成を示すブロック図である。PC102は、CPU110、デバイス111aや制御プログラム111b等を予め記憶しているROM111、RAM112、ディスプレイ103、通信回線101と接続するためのモデムポートやプレーヤ201と接続するためのUSB等を備える通信ポート113、キーボード104、内部バス114、メモリカード109と内部バス214とを接続するメモリカードライタ107、メモリカード109から読み出された時系列化音楽データを復号するMPPEG2117、復号された音楽データを伸張するMPPEG2-AAC（ISO13818-7）に準拠したAACデコーダ118、伸張されたデジタル音楽データをアナログ信号に変換するD/Aコンバータ119、スピーカ106及びファイル管理ソフトウェアやアプリケーションを格納しているハードディスク120等から構成される。

【0022】図5は、メモリカード109の外観及びハードウェア構成を示す図である。メモリカード109は、何度も繰り返し返り行われる書き換え可能な不揮発性メモリを内蔵しており、その記憶容量は64MBであり、外部から3.3Vの電源とクロック信号の供給を受けて動作する。また、メモリカード109は、厚さ2.1mm、縦32mm、横24mmの立方体形状で、その側面に書き込み防止スイッチ（ライトプロテクトSW）を有し、9ピンの接続端子によって電気的に外部機器と接続される。

【0023】このメモリカード109は、3つのICチップ（コントロールIC302、フラッシュメモリ303、ROM304）を内蔵している。フラッシュメモリ303は、一括消去型の書き換え可能な不揮発メモリであり、物理的な記憶領域として、正当な機器であると認識することができた機器に対してアクセスを許可する記憶領域である記憶領域332と、そのような記憶を必要とすることなくアクセスを許可する記憶領域である非記憶領域331等を有する。ここでは、記憶領域332は、著作権保護に関わる重要なデータを格納するために用いられ、非記憶領域331は、一般的なコンピュータシステムにおける補助記憶装置として用いられる。なお、これらの2つの記憶領域は、フラッシュメモリ303上の一定のアドレスを境界として区分されている。【0024】ROM304は、特殊領域と呼ばれる読み出し専用の記憶領域を有し、このメモリカード109に固有の識別情報であるメディアID341やこのメモリカード109の製造メーカー名342等の情報を予め保持している。なお、メディアID341は、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データであり、ここでは、機器間の相互認証に用いられ、記憶領域332への不正なアクセスを防止するために使用される。

【0025】コントロールIC302は、アクティブ素子（制御ゲート等）からなる制御回路であり、記憶領域321、コマンド判定制御部322、マスター記憶領域323、特殊領域アクセス制御部324、記憶領域アクセス制御部325、非記憶領域アクセス制御部326及び時系列化音楽データ327等を有する。記憶領域321は、このメモリカード109にアクセスしようとする相手機器とチャレンジャー・レスポンス型の相互認証を行う回路であり、乱数発生器や暗号器等を有し、その暗号器と同一の暗号器を相手機器が有しているか否かを検出することによって、相手機器の正当性を認証する。なお、チャレンジャー・レスポンス型の相互認証とは、相手機器の正当性を検証するためにチャレンジャーは相手機器に送る、それに対して相手機器において自己の正当性を証明する処理が施こされて生成されたレスポンスデータを相手機器から受け取り、それらチャレンジャーデータとレスポンスデータとを比較することで相手機器を認証することがで

きるかを判断するという認証ステップを、双方の機器が相互に行うことである。

【0026】コマンド判定制御部322は、コマンドと9への命令）の種類を判定し実行するデコード回路や制御回路からなるコントロールローラであり、入力されたコマンドの種類に応じて、各種構成要素321～327を制御する。コマンドには、フラッシュメモリ303のデータを読み書き・消去するコマンドだけでなく、フラッシュメモリ303を制御するためのコマンド（7アドレス空間や未消去データに関するコマンド等）も含まれる。

【0027】例えば、データの読み書きに関しては、記憶領域332にアクセスするためのコマンド「SecureRead address count」や、非記憶領域331にアクセスするためのコマンド「Read address count」、「Write address count」等が定義されている。ここで、「address」は、読み書きの対象となる一連のセクタ群の最初のセクタの番号であり、「count」は、読み書きする合計セクタ数を示す。また、セクタは、メモリカード109に対してデータを読み書きする際の単位であり、ここでは、512バイトである。

【0028】マスター記憶領域323は、相互認証の際に相手機器が用いたり、フラッシュメモリ303内のデータを保護するために用いられるマスター鍵323aを予め記憶している。特殊領域アクセス制御部324は、特殊領域（ROM304）に格納されたメディアID341等を読み出す回路である。

【0029】記憶領域アクセス制御部325及び非記憶領域アクセス制御部326は、それぞれ、フラッシュメモリ303の記憶領域332及び非記憶領域331へのデータ書き込み及び読み出しを実行する回路であり、4本のデータピンを介して外部機器（PC102やプレーヤ201等）との間でデータを送受信する。なお、これらアクセス制御部325、326は、内部に1ブロック分のパッドメモリを有し、論理的には（外部機器とのコマンド上でのアクセスは）セクタを単位として入力するが、フラッシュメモリ303の内容を書き換えるときには、ブロック（32個のセクタ、10Kバイト）を単位として入力する。具体的には、ある1個のセクタデータを書き換える場合には、フラッシュメモリ303から該当するブロックをバッファメモリに読み出し、そのブロックを一括消去するとともに、バッファメモリ中の該当セクタを書き換えた後に、そのブロックをバッファメモリからフラッシュメモリ303に書き戻す。

【0030】時系列化音楽データ327は、記憶領域アクセス制御部325及び非記憶領域アクセス制御部326による制御の下で、マスター記憶領域332に格納されたマスター鍵323aを用いて時系列化及び復号化を行う回路であり、フラッシュメモリ303にデータを書き込

領域にそのデータを暗号化して書き込み、フラッシュメモリ303からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがそのメモ리카ード109を分解してフラッシュメモリ303の内容を直接解析し、暗証領域332に格納されたパスワードを盗む等の不正行為を防止するためである。

【0031】なお、コントロールIC302は、これら主要な構成要素321～327の他に、クロック信号から供給されるクロック信号に同期した内部クロック信号を生成し各構成要素に供給する同期回路や、駆動性の記憶領域及び不揮発性の記憶領域等を有する。また、特殊領域(ROM304)に格納されている情報の改ざんを防止するために、そのROM304をコントロールIC302の中に内蔵させた。それらの情報をフラッシュメモリ303に格納し、外部から書き込みできないように特殊領域アクセス制御部324が制限をかけてもよい。そのときに、暗号・復号化回路327で暗号化したデータを格納することとしてもよい。

【0032】図6は、PC102やプレーヤ201から見たメモ리카ード109の記憶領域の構成を示す図である。メモ리카ード109が有する記憶領域は、大きく分けて、特殊領域304と暗証領域332と非暗証領域331の3つの領域である。特殊領域304は読み出し専用の領域で、この中のデータに対しては、専用コマンドを用いて読み出しを行う。暗証領域332は、PC102又はプレーヤ201とメモ리카ード109との間で暗証が成功した時にのみ読み書きができる領域で、この領域へのアクセスについては暗号化されたコマンドを用いる。非暗証領域331は、ATAやSCSI等の公開されたコマンドでアクセスできる。即ち、暗証領域331に読み書きできる領域である。従って、非暗証領域331に対しては、フラッシュATAやコンパクトフラッシュと同一ように、PC102上のファイル管理ソフトウェアでデータの読み書きが可能である。

【0033】3つの記憶領域には、以下の情報を格納することとし、これによって、一般的なPCの補助記憶装置として格納部と、電子音楽記憶に係る音楽データに対する著作権保護の機能とを提供している。つまり、非暗証領域331には、著作権保護の対象となる音楽データが暗号化された暗号化コンテンツ426や、著作権保護と無関係な一般的なデータであるユーザデータ427等が格納される。暗証領域332には、非暗証領域331に格納された暗号化コンテンツ426を復号するための秘密鍵となる暗号化キー425が格納される。そして、特殊領域304には、暗証領域332にアクセスするために必要とされる情報であるメディアID341が格納されている。

【0034】PC102やプレーヤ201は、まず、装着されたメモ리카ード109の特殊領域304に格納されたメディアID341を読み出し、それを用いて暗証

領域332に格納された暗号化キー425、権利情報を取り出す。それら暗号化キー425と権利情報によって再生が許可されていれば、非暗証領域331にある暗号化コンテンツ426を読み出し、暗号化キー425で復号しながら、再生を行うことができる。

【0035】もし、あるユーザが不正に入手した音楽データだけをPC102等でメモ리카ード109の非暗証領域331に書き込み、そのようなメモ리카ード109をプレーヤ201に装着して再生しようとしたとする。しかし、そのメモ리카ード109の非暗証領域331に音楽データが格納されているものの、暗証領域332に対応する暗号化キー425と権利情報が存在しないために、そのプレーヤ201は、その音楽データを再生することができない。これによって、正規の暗号化キーや権利情報を伴わないで音楽コンテンツだけをメモ리카ード109に複製しても、その音楽コンテンツは再生されない。このため、デジタル著作権物の不正な複製が防止される。

【0036】図7は、PC102やプレーヤ201がメモ리카ード109の各領域にアクセスする際の制限やコマンドの形態を示す図であり、(a)は各領域へのアクセスにおけるルールを示し、(b)は各領域のサイズの変更におけるルールを示し、(c)はメモ리카ード109の領域を示す概念図である。特殊領域304は、読み出し専用の領域であり、暗証せずに専用コマンドでアクセスできる。この特殊領域304に格納されたメディアID341は、暗証領域332にアクセスするための暗号化コマンドの生成や復号に用いられる。つまり、PC102やプレーヤ201は、このメディアID341を読み出し、これを用いて暗証領域332にアクセスする。その暗号化コマンドを受けたメモ리카ード109は、メディアID341を用いて、その暗号化コマンドを復号し、解釈して実行する。

【0037】暗証領域332は、PC102やプレーヤ201等のメモ리카ード109にアクセスする装置とメモ리카ード109との間で暗証が成功した時にのみアクセスが可能となる領域であり、その大きさは(YYY+1)個のセクタに相当する。つまり、この暗証領域332は、論理的には、第0～YYYのセクタで構成され、物理的には、フラッシュメモリ303の第XXX～第(X+YYY+1)のセクタアドレスを有する。ランダムメモリ303を構成する全てのセクタそれぞれに対してユニークに付された一連の番号のことである。【0038】非暗証領域331は、暗証せずにATAやSCSI等の標準コマンドでアクセスすることが可能で、その大きさはXXX個のセクタに相当する。つまり、この非暗証領域331は、論理的にも物理的にも第0～(XXX-1)のセクタで構成される。なお、フラッシュメモリ303には、暗証領域332や非暗証領域

領域を変更すればよい。これによって、暗証領域332に格納されていたデータの論理アドレスを維持したまま、そのデータ空間が拡大される。

【0044】なお、領域変更のための専用コマンドについても、不正なアクセスを防止する観点から、コマンドを暗号化して用いることとしてもよい。図8は、音楽データ等のコンテンツをPC102(及びプレーヤ201)がメモ리카ード109に書き込む動作を示すフロー図である。ここでは、PC102がメモ리카ード109へ書き込む場合(S601)を説明する。

【0045】(1) PC102は、デバイスID111a等を用いて、メモ리카ード109の暗証部321とチャレンジ・レスポンス型の暗証を行い、その暗証に成功すると、まず、メモ리카ード109からマスター鍵323aを取り出す(S602)。(2) 次に、専用コマンドを用いて、メモ리카ード109の特殊領域304に格納されているメディアID341を取り出す(S603)。

【0046】(3) 続いて、乱数を生成し、その乱数20と、いま取り出したマスター鍵323aとメディアID341とから、音楽データを暗号化するためのパスワードを生成する(S604)。このときの乱数は、例えば、上記暗証において、メモ리카ード109に送信したチャレンジデータ(乱数)を暗号化したものを用いる。

(4) 得られたパスワードをマスター鍵323aとメディアID341で暗号化し、暗号化キー425として暗証領域332に書き込む(S605)。このときには、暗証領域332に書き込む暗号化キー425を暗号化してメモ리카ード109に送信しておく。

【0047】(5) 最後に、音楽データをパスワードで暗号化しながら暗号化コンテンツ426として非暗証領域331に格納していく(S606)。図9は、音楽データ等のコンテンツをメモ리카ード109から読み出し、プレーヤ201(及びPC102)で再生する動作を示すフロー図である。ここでは、メモ리카ード109内の音楽データをプレーヤ201が再生する場合(S701)を説明する。

【0048】(1) プレーヤ201は、デバイスID211a等を用いて、メモ리카ード109の暗証部321とチャレンジ・レスポンス型の暗証を行い、その暗証に成功すると、まず、メモ리카ード109からマスター鍵323aを取り出す(S702)。

(2) 次に、専用コマンドを用いて、メモ리카ード109の特殊領域304に格納されているメディアID341を取り出す(S703)。

(3) 続いて、メモ리카ード109の暗証領域332から音楽データの暗号化キー425を取り出す(S704)。このときには、データ(暗号化キー4

暗証領域332に格納された暗号化キー425、権利情報を取り出す。それら暗号化キー425と権利情報によって再生が許可されていれば、非暗証領域331にある暗号化コンテンツ426を読み出し、暗号化キー425で復号しながら、再生を行うことができる。

【0039】また、特殊領域304は暗証なしでアクセスできるとしたが、不正なユーザからの解析を防ぐために、暗証を行ってからでないとアクセスできないとしてよいし、特殊領域304にアクセスするコマンドを暗号化してよい。次に、図7(b)及び(c)を用いて、暗証領域332と非暗証領域331それぞれの領域サイズを変更する方法について説明する。

【0040】フラッシュメモリ303に設けられる暗証領域332と非暗証領域331との合計の記憶容量は、フラッシュメモリ303の全記憶領域から代替ブロック領域501等を除いた固定値、即ち、(XXX+YY+YY+1)個のセクタ分であるが、それぞれの大きさは、境界アドレスXXXの値を変更することで、可変となっている。

【0041】領域の大きさを変更するためには、最初に暗証を行う。これは、PCのユーザに広く開示されている標準プログラムや不正なアクセスを行うソフト等を用いて領域の大きさを変更することができないようにするためである。暗証を行った後は、領域変更の専用コマンドで、非暗証領域331の大きさ(新たなセクタ数XXX)をメモ리카ード109に送る。

【0042】メモ리카ード109は、その領域変更コマンドを受け取ると、その値XXXXをメモ리카ード109内の不揮発性記憶領域等に保持し、以降のアクセスにおいては、その値を新たな境界アドレスとして、暗証領域332及び非暗証領域331へのアクセス制御を実行する。つまり、フラッシュメモリ303上の物理的なセクタ0～XXXのセクタを非暗証領域331に割り当てるとともに、第XXXX～(XXXX+YYY)番目のセクタを暗証領域332に割り当てる。そして、そのような新たなメモリアッピングに基づいて、アクセス制御部325及びメモリマッピングに基づいて、アクセス制御を監視したり、領域を超えるアクセス違反の発生を監視したりする。なお、暗証アドレスとは、外部機器からメモ리카ード109を見た場合の(コマンド上の)データ空間におけるアドレスであり、物理アドレスとは、メモ리카ード109のフラッシュメモリ303が有するデータ空間におけるアドレスである。

【0043】ここで、もし、境界アドレスを小さくすることにより、暗証領域332のサイズを大きくした場合には、変更前との論理的な互換性を維持するために、暗証領域332に格納されていた全てのデータを移動させる等の手当てが必要となる。そのためには、例えば、境界アドレスの移動量だけアドレスの下方方向に全データを移動( Shift )させ、新たな境界アドレスから始まる論理アドレスに新たな物理アドレスが対応するように対応

25) の読み出しに先立ち、認証領域 332 から読み出すためのコマンドを暗号化してメモリカード 109 に送信しておく。

15

【0050】(5)最後に、非保証領域331から暗号化コンテンツ426を読み出し、上記ステップS705で抽出したパスワードで復号し、それが暗号を再生している

く(5708)。このように、メモリカード109の押印領域331に特許された音楽データは、配位領域332の暗号化キー425がないと復号することができない。従って、たとえ不正に音楽データだけを別のメモリカードにコピーしたとしても、その音楽データを正常に再生することができないので、その音楽データの著作権は安全に保護される。

【0051】また、図2に成功した機器だけがメモリアルカードの認証領域へのアクセスが許可されるので、認証に用いられるデバイス鍵や暗号化アルゴリズム等を適切に選択して用いることで、一定の条件を満たした機器だけに對してメモリアルカードの認証領域へのアクセスを許可する等の著作権保護が可能となる。なお、この例では、メモリアルカード109に暗号化コンテンツを記録する際に、その暗号化に用いられるマスターワードをマスター鍵とメディアIDで暗号化し、暗号化キーとして認証領域332に格納されたものが（S605）、マスター鍵及びメディアIDのいずれかを用いて暗号化することとしてもよい。これによつて、暗号の強度が低下する恐れがあるものの、暗号化の規格に依り、メモリアルカード109やプレーヤ201等の回路規模が小さくなるという利点が得られる。

【0052】また、プレーヤ201やPC102は、図1に示すように、メモリカード109からマスター鍵323aを取り出し、メモリカード109からマスター鍵323aを取り出したが、プレーヤ201やPC102にそのマスター鍵323aを埋め込んでおいてもよいし、マスター鍵323aを暗号化し、暗号化マスター鍵として特殊領域304に格納しておいてもよい。次に、このようなメモリカードの既述箇様の活用例として、「版出し回数」を格納した例と、「デジタル出力許可回数」を格納した例を示す。

【0053】図10は、プレーヤ201及びPC102が出し回されたカード109の対応位置に格納された読み出し回数812を操作する動作を示すフロー図である。ここでは、メモリア2109に格納された読み出し回数812の範囲内のみ、プレーヤ201が、メモリア2109の非対応位置331に格納された音楽データを音流信号に再生することが許可されている場合(5801)について説明する。

【0054】(1) プレーヤ201は、デバイス鍵21

再生の場合 (S701~S705) と同様にして、メモ  
リカード109と認証を行なった後にマスタ一鍵323  
aを取り出し (S902)、メディアID341を取り  
出し (S903)、暗号化キー425を取り出す (S9  
04)、パスワードを抽出する (S905)。

(2) 次に、メモリアカード10.9の保証領域332からデジタル出力許可回数9.3を取り出し、その値を検査する(S906)。その結果、その値が無制限なデジタル出力出力を許可する旨の値である場合は、非保証領域333から暗号化コンテンツ42.6を読み出し、上記ステップS905で抽出したパスワードで復号しながらデジタル音楽データとしてデジタル出力端子20.5から出力する(S909)。

【0061】(3) 一方、デジタル出力許可回数913が0を示す場合は、もはやデジタル出力は許可されていないと判定し(S908)、アナログ出力による再生だけを行なう(S908)。つまり、非総置換域331から暗号化コンテンツ426を読み出し、バスワードで復号しながら音楽を再生する(S908)。

(4) 読み出したデジタル出力許可回数913が0では  
ない一定の制限回数を表示する場合は、その回数を1つ減算  
し、その結果を記憶域332に書き戻した後に(S9  
07)、非閉じ領域331から符号化コンテンツ426  
を読み出し、上記ステップS905で抽出したパター  
ンで復号しながらデジタル出力用の音源データとしてデジタル  
出力端子205から出力する(S909)。

【0062】このように、メモ리카ード109の記憶領域332に、予め付与されたデジタル出力の回数指定したデジタル出力許可回数913を格納しておくことにより、ブレイク201による音楽データのデジタル出力の回数をコントロールすることが可能となる。これによって、例えば、レンタルCDやKIOSK端末等によるデジタル再生への適用、即ち、メモ리카ードに記憶した音楽データのデジタルダビングを著作権者の了解の示に指定した回数分だけコピーを許可するような運用が実現となる。

【0063】なお、「野み出し回教」の場合と同様に、デジタル出力許可回数913に代えて、「デジタル出力許可時間」とすることで、音楽コンテンツをデジタルデータのまま出力することが可能な組込み制限することでもできる。また、回教と時間とを組み合わせてもよい。たとえば、デジタル出力許可回教913は、その出力を開始してから10秒毎の一定時間を超えて出力され続けた場合にだけ、その回教を減算してもよい。また、デジタル出力許可回教913は、不正な改ざんを防ぐために暗号化して登録することとしてもよい。

【0064】さらに、著作権者に代金を払い込むことで、著作権者が指定した回数だけデジタル出力許可回数を増やす機能を追加してもよい。次に、このメモ리카ード109の物理的なデータ構造（セクタ及びECCブロック）について説明する。

ックの構造)について説明する。このメモモリカード1019では、フラッシュメモリ313の32に格納されたデータのバッドアツクと復元に伴う不正行為やデータの改ざんに伴う不正行為等を防止するに好適なデータ構造が採用されている。つまり、上述のような「読み出し回数」や「デジタル出力計可回数」を記憶回路312に格納し、それらを行爲を実行する際にカウンタダウンしていく方式では、次のような攻撃を受ける可能性がある。

【0065】つまり、フレンジュメモリ303全体の配  
10 置データを外部の補助記憶装置等にバックアップしてお  
いた後に音楽再生を繰り返し、それら回数が0となり、再び  
時点でバックアップデータを復元する回数により、再び  
音楽再生を繰り返したり、「読み出し回数」そのものを  
改ざんすることで、不正に音楽再生を繰り返すことが考  
えらる。従って、そのような行為を防止する手段が必要となる。

【0066】図12は、メモリカード109の記憶領域332及び非記憶領域331に共通のデータ構造と、そのデータ構造に対応した読み書き処理のフローとを示す図である。ここでは、コントロールC302の記憶部321等に有する乱数発生部1003が発生するランダム値が時変の値として利用される。

【0067】フラッシュメモリ303には、512バイトのセクタ1004ごとに、16バイトの拡張領域1005が割り当てられる。各セクタは、カウンタ値で暗号化されたデータが格納される。拡張領域1005は、対応するセクタに格納されている暗号化データの誤り訂正符号を格納するための8バイトのECCデータ1006と、その暗号化データの生成に用いられたカウンタ値を格納するための8バイトの時定領域1007とからなる。

【0068】なお、数理的に（ユニザ）に開放されたコマンド等を用いて、アクセス可能な領域はセクタ1004だけであり、拡張領域1005は、物理的に（メモ리카ードを読み書きする装置による制御として）のみアクセス可能な領域である。このようなデータ構造とすることで、コマンド等を用いてセクタデータだけが改ざんされても、暗装領域1007の内容は改ざんされることはない。そのため、それらの整合性を利用することで、不正な改ざんを防止することができ、

【0069】具体的に、PC102やプレーヤ201は、セクタ1004ごとに、以下の手順に従って、フラッシュメモリ303の記憶領域332と非検証記憶331にデータを格納したり、読み出したりする。ここで、まず、PC102がメモリ109にデータを、符を含む場合（S1001）の手順を説明する。

(1) PC102は、メモリカード109に対してカード10の値の発行を要求する。すると、メモリカード109内のコントロールIC302は、内部の乱数発生器150003で乱数を発生し(S1005)、その乱数をタウ

19  
ンター値としてPC102等へ送る(S1002)。  
[0070] (2) 取得したカウンタ値と、既に取得したカウンタ値323a及びメディアID341とからバスワードを生成する(S1003)。  
(3) 書き込むべき1セクタ分のデータをバスワード暗号化しながら、メモリアード109に送る(S1004)。このとき、書き込むべきセクタを指定する情報や、暗号化に用いたカウンタ値も一緒に送る。  
(4) メモリアード109は、受け取った暗号化データを、指定されたセクタ1004に書き込む(S1006)。  
[0071] (5) その暗号化データからECCを計算し、上記セクタに対応する拡張領域1005に、ECCデータ1006として書き込む(S1007)。  
(6) 続いて、上記暗号化データとともに受け取ったカウンタ値を拡張領域1007に書き込む(S1008)。  
(7) 次に、PC102がメモリアード109からデータを読み出す場合(S1011)の手順を説明する。  
[0072] (1) PC102は、メモリアード109に対して、セクタを指定するとともにデータの読み出しを要求する。すると、メモリアード109は、まず、指定されたセクタ1004の暗号化データだけを読み出してPC102に出力し(S1016)、PC102は、そのカウンタの暗号化データを受け取る(S1012)。  
(2) 次に、メモリアード109は、指定されたセクタ1004に対応する拡張領域1005の時定領域1007に格納されたカウンタ値を読み出してPC102に出力し(S1017)、PC102は、そのカウンタ値を受け取る(S1013)。  
[0073] (3) 読み出したカウンタ値と、既に取得したマスナー値323a及びメディアID341とからバスワードを生成する(S1014)。  
(4) そのバスワードを用いて、暗号化データを復号する(S1015)。ここで、もし、不正な改ざん等により、セクタ1004のデータが変更されている場合には、時定領域1007から読み出されたカウンタ値と、セクタ1004のデータが変更されている場合に、ユーザからは見えない(アクセスできない)領域としての時定領域1007を設け、そこに格納されたカウンタ値に依存したバスワードでデータの改ざんを格納すること、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時定領域1007は、ECCを格納するための拡張領域1005として、メモリアードの外側から書き換えがでない領域であられ、フラッシュメモリ303内の他の領域に設けられている。  
[0074] このように、フラッシュメモリ303内に、ユーザからは見えない(アクセスできない)領域としての時定領域1007を設け、そこに格納されたカウンタ値に依存したバスワードでデータの改ざんを格納すること、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時定領域1007は、ECCを格納するための拡張領域1005として、メモリアードの外側から書き換えがでない領域であられ、フラッシュメモリ303内の他の領域に設けられている。

20  
き換える機能を有する。具体的には、コントロールIC303の命令制御部322は、交換テーブル1101を書き換えるための専用コマンドがコマンドピンから入力される。そのコマンドを解釈し、続いて送られてくるパラメータを用いて交換テーブル1101を書き換える。  
[0081] その具体的な動作は、図13に示される通りである。いま、上記専用コマンドが送られてくる前にあるのは、フラッシュメモリ303において、図13(a)に示されるように、物理アドレス0及び2にファイルfilloを構成するデータが存在し、物理アドレス1にファイルfillo2を構成するデータが存在する。そして、交換テーブル1101には、図13(c)に示されるように、物理アドレスと論理アドレスとが一致する内容が保持されている。つまり、物理アドレスと上と同様に、論理アドレス上においても、ファイルfilloのデータが別のファイルfilloのデータに換わって格納されていること。

21  
[0082] このよう状態を解消しようとする外部機器は、フラッシュメモリ303に対して、特定のファイルfilloの連続性を確保する旨を示す上記専用コマンド及びパラメータを送る。すると、メモリアード109は、コマンド判定部322は、その専用コマンド及びパラメータに従って、交換テーブル1101を、図13(d)に示される内容に書き換える。つまり、フラッシュメモリ303の論理アドレスと物理アドレスの対応関係は、図13(b)に示されるように変更される。  
[0083] 図13(b)に示された関係図から分かるように、物理アドレスの配置は変化していないにもかかわらず、ファイルfilloを構成する2つの論理ブロックが逆接するように再配置されている。これによって、その外部機器は、次のアクセス以降においては、それまでよりも高速にファイルfilloにアクセスすることが可能となる。

22  
[0084] 以上のような交換テーブル1101の変更は、論理ブロックのフラグメンテーションを解消するだけでなく、フラッシュメモリ303の拡張領域332と非拡張領域331それぞれのサイズを変更する場合にも用いられる。このときは、サイズを小さくする領域の物理ブロックがサイズを大きくする領域の物理ブロックとして割り当てられるように交換テーブル1101を書き換えるだけで済むので、高速な領域変更が可能となる。  
[0085] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

22  
される(書き込まれる)前に一括消去が必要とされる物理ブロックである。  
[0086] また、未消去リストコマンドとは、コマンド判定部322が解釈及び実行可能なコマンドのひとつであり、その時点におけるフラッシュメモリ303に存在する全ての未消去ブロックの番号の一覧を取得するためのコマンドである。メモリアード109に使用されているフラッシュメモリ303は、書き込みを行う前にブロック単位で一括消去が必要とされるが、その消去処理は書き込み時間の半分近くを占めるため、予め消去しておいた方がより高速に書き込むことができる。そこで、このメモリアード109は、その便宜を図るために、未消去リストコマンドと消去コマンドを外部機器に提供している。

23  
[0087] いま、フラッシュメモリ303は、図14(a)に示されるような論理ブロック及び物理ブロックの使用状態とする。ここでは、論理ブロック0~2が使用中であり、物理ブロック0~2、4及び5が未消去ブロックとなっている。この状態においては、コマンド判定部322内に保持されている未消去リスト1203は、図14(b)に示される内容となっている。ここで、未消去リスト1203は、フラッシュメモリ303を構成する全ての物理ブロックに対応するエンTRIESとなる記憶テーブルであり、コマンド判定部322による制御の下で、対応する物理ブロックの消去状態に応じた値(消去済みの場合は“0”、未消去の場合は“1”)が保持される。

24  
[0088] 図14(c)は、このような状態においてPC102がブレイク201が未消去リストコマンドと消去コマンドを用いて事前にブロックを消去する場合の動作を示すフロー図である。なお、フラッシュメモリ303には、図14(d)に示されるように、論理ブロックの使用状態を示すFAT (File Allocation Table)等のテーブルが格納されているものとする。

25  
[0089] PC102がブレイク201等の外部機器は、例えば、メモリアード109へのアクセスが発生していないアイドル時間において、このメモリアード109に対して未消去リストコマンドを実行する(S1201)。そのコマンドを受け取ったメモリアード109の命令制御部322は、内部に有する未消去リスト1203を参照することで、状態値1が登録されている物理ブロックの番号0~2、4及び5を特定し、その外部機器に返す。

26  
[0090] 続いて、外部機器は、フラッシュメモリ303に格納された図14(d)に示される論理ブロックの使用状態を示すテーブルを参照することで、論理的に使用されていないブロックを特定する(ステップS1202)。そして、上記2つのステップS1201及びS1202で取得した情報に基づいて、消去可能なブロック、即ち、論理的に不使用で、かつ、物理的に未消去な

27  
[0091] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

28  
[0092] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

29  
[0093] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

30  
[0094] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

31  
[0095] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

32  
[0096] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

33  
[0097] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

34  
[0098] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

35  
[0099] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

36  
[0100] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

37  
[0101] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

38  
[0102] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

39  
[0103] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

40  
[0104] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

41  
[0105] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

42  
[0106] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

43  
[0107] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

44  
[0108] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

45  
[0109] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

46  
[0110] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

47  
[0111] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

48  
[0112] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

49  
[0113] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

50  
[0114] 次に、このメモリアード109が有する未消去ブロックに関する機能。具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ303内の物理ブロックであって、過去に書き込みが行われ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用

ブロック（ここでは、物理ブロック4と5）を特定した後に（ステップS1203）、メモリカード109に対して、それらブロック4と5の番号を指定した消去コマンドを実行する（ステップS1204）。そのコマンドを受信したメモリカード109の制御部325、326に指示を出す等により、指定された物理ブロック4と5を一括消去する。

【0091】これによって、もし、その物理ブロック4と5への書き込みが発生した場合には、その物理ブロックに対する消去処理は不要となるので、高度な書き込みが可能となる。次に、このメモリカード109が有する個人データの保護に関する機能、具体的には、メモリカード109が外部機器を認証する際にその外部機器を使用するユーザの個人データを必要とする場合における個人データの保護機能について説明する。ここで、個人データとは、そのユーザを一意に識別するためのデータであって、メモリカード109の認証領域332へのアクセスが許可されるためのデータとしてメモリカード109に記憶させるためのデータである。

【0092】このような場合において、認証領域332へのアクセスの際にユーザに対して繰り返し個人データを入力することを要求したり、その個人データを認証領域332に格納することとは、不正者によって盗取された、認証領域332にアクセスする権限を有する他のユーザによって見られたために、音楽データと同様（0093）これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで暗号化してから格納するという方法が考えられる。しかしながら、パスワードを設定した場合には、その個人データを見るたびにパスワードを入力しなければならず、手続が面倒であり、その管理も必要となる。そこで、このメモリカード109は、不必要に個人データを繰り返し入力することを回避する機能を有する。

【0094】図15は、認証のためのプレーヤ201とメモリカード109間の通信シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ201の認証領域216及びメモリカード109の認証部321によって実現される。本図に示されるように、プレーヤ201の認証領域216は、暗号化及び復号化等の機能の他に、メモリカード109に保持されたマスター鍵323aと同一の秘密鍵であるマスター鍵1301と、製造番号（s/n）等のプレーヤ201に固有のIDである機器固有ID1302とを予め記憶している。

【0095】また、メモリカード109の認証部321は、暗号化、復号化及び比較等の機能の他に、2つの不揮発性記憶領域である機器固有ID群記憶領域1310とユーザキー記憶領域1311とを有する。機器固有ID群記憶領域1310は、このメモリカード109の認

証領域332へのアクセスが許可された全ての機器の機器固有IDを記憶しておくための記憶領域であり、ユーザキー記憶領域1311は、個人データとして機器から送られてきたユーザキーを記憶しておくための記憶領域である。

【0096】具体的な認証手順は、以下の通りである。なお、送受信においては、全てのデータは暗号化されて送受信され、受信側で復号される。そして、手順が進む度に、次の手順での暗号化及び復号化に用いられる鍵が生

成される。

(1) メモリカード109とプレーヤ201とを接続すると、まず、プレーヤ201は、マスター鍵1301を用いて機器固有ID1302を暗号化し、メモリカード109に送る。

【0097】(2) メモリカード109は、受け取った暗号化された機器固有ID1302をマスター鍵323aで復号し、得られた機器固有ID1302が既に機器固有ID群記憶領域1310に格納されているか検査する。

(3) その結果、既に機器固有ID1302が格納されている場合は、認証が成功した旨をプレーヤ201に通知し、一方、機器固有ID1302が格納されていない場合は、プレーヤ201に対しユーザキーを要求する。

【0098】(4) プレーヤ201は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリカード109に送る。

(5) メモリカード109は、送られてきたユーザキーと予めユーザキー記憶領域1311に格納されているものとを比較し、一致している場合、又は、ユーザキー記憶領域1311が空であった場合は、認証が成功した旨をプレーヤ201に通知するとともに、上記ステップ(3)で獲得した機器固有ID1302を機器固有ID群記憶領域1310へ格納する。

【0099】これによって、ユーザが所有する機器とメモリカード109とを初めて接続した場合は個人データ（ユーザキー）の入力が必要とされるが、2回目以降には認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メモリカード109とPC102やプレーヤ201等の外部機器との認証プロトコルの変形例について、図16及び図17を用いて説明する。

【0100】図16は、変形例に係るメモリカード109と外部機器（ここでは、プレーヤ201）との認証手順を示す通信シーケンス図である。この処理は、主に、変形例に係るプレーヤ201の認証領域216、PC102の制御プログラム111b及びメモリカード109の認証部321によって実現される。また、メモリカード109のマスター鍵記憶領域323には、暗号化さ

れたマスター鍵（暗号化マスター鍵323b）が格納されており、暗号領域304には、メディアID341に加えて、そのメディアID341を暗号化して得られるセキュアメディアID343も格納されているものとす

る。

【0101】まず、プレーヤ201は、メモリカード109にコマンドを送ることで、メモリカード109のマスター鍵323bを取り出し、デバイス鍵211aで復号する。この復号アルゴリズムは、メモリカード109に格納されている暗号化マスター鍵323bが生

成された際に用いられた暗号アルゴリズムに対応する。従って、このプレーヤ201が有するデバイス鍵211aが予定されたもの（正規のもの）であれば、この復号によって元のマスター鍵に復元される。

【0102】続いて、プレーヤ201は、メモリカード109にコマンドを送ることで、メモリカード109のメディアID341を取り出し、復元された上記マスター鍵で暗号化する。この暗号アルゴリズムは、メモリカード109に格納されているセキュアメディアID343が生成された際に用いられた暗号アルゴリズムと同一である。従って、この暗号化によって、メモリカード109が有するセキュアメディアID343と同一のセキュアメディアIDが得られる。

【0103】続いて、それらセキュアメディアIDそれぞれを用いて、プレーヤ201とメモリカード109とは、相互認証を行う。その結果、いずれの機器においても、相手機器の認証に成功したか否かを示す（OK/NG）情報と、その認証結果に依存して定まる暗号の鍵であるセキュア鍵とが生成される。このセキュア鍵は、双方の機器201及び109が認証に成功した場合にのみ一致し、かつ、相互認証を繰り返す度に異なる性質を有する。

【0104】続いて、相互認証に成功すると、プレーヤ201は、メモリカード109の認証領域332にアクセスするためのコマンドを生成する。具体的には、例えば、認証領域332からデータを読み出す場合であれば、そのコマンド「SecureReadaddress count」のバリエータ（24ビット長のアドレス「address」と8ビット長のカウンタ「count」）をセキュア鍵で暗号化し、得られた暗号化バリエータと、そのコマンドのタグ（コマンドの種類「SecureRead」を示す8ビット長のデータ）とを連結して得られる暗号化コマンドをメモリカード109に送る。

【0105】暗号化コマンドを受け取ったメモリカード109は、そのタグからコマンドの種類を判定する。ここでは、認証領域332からの読み出しコマンド「SecureRead」であると判定する。その結果、認証領域332へのアクセスコマンドであると判定した場合には、そのコマンドに含まれていたバリエータを、相互認証で得られたセキュア鍵で復号する。この復号アルゴリズム

は、プレーヤ201において暗号化コマンドを生成する際に用いられた暗号アルゴリズムに対応するもので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるバリエータは、プレーヤ201で用いられた元のバリエータに等しくなる。

【0106】そして、メモリカード109は、復号されたバリエータによって特定されたセクタに格納された暗号化キー425を認証領域332から読み出し、それをセキュア鍵を用いて暗号化しプレーヤ201に送信する。プレーヤ201は、送られてきたデータを、相互認証で得られたセキュア鍵を用いて復号する。この復号アルゴリズムは、メモリカード109において暗号化キー425の暗号化に用いられたアルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるデータは、元の暗号化キー425に一致する。

【0107】なお、メモリカード109は、認証領域332へのアクセスコマンドの実行を終える度に、それを用いたセキュア鍵を破棄（消去）する。これによって、メモリカード109の認証領域332にアクセスする外部機器は、1回のコマンドを送出する度に、毎回相互認証を行い、それにパスしている必要がある。図17は、図16に示された相互認証における詳細な手順を示す通信シーケンス図である。ここでは、メモリカード109とプレーヤ201は、チャレンジ・レスポンス型の相互認証を行う。

【0108】メモリカード109は、プレーヤ201の正当性を検証するために、乱数を生成し、それをチャレンジデータとしてプレーヤ201に送る。プレーヤ201は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてメモリカード109に送る。メモリカード109は、そのレスポンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、プレーヤ201の認証に成功した（OK）と認識し、そのプレーヤ201から送られてくる認証領域332へのアクセスコマンドを受け付ける。一方、比較の結果、一致しなかった場合には、認証に成功しなかった（NG）したと認識し、もし、その後にプレーヤ201から認証領域332へのアクセスコマンドが送られてきたとしても、その実行を拒絶する。

【0109】同様にして、プレーヤ201は、メモリカード109の正当性を検証するために、上記認証と同様のやりとりを行う。つまり、乱数を生成し、それをチャレンジデータとしてメモリカード109に送る。メモリカード109は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてプレーヤ201に送る。プレーヤ201は、そのレスポ



31  
ズ変更回路は、前記一定サイズの記憶領域を2分する境界アドレスを変更することによって前記記憶領域及び前記非記憶領域をそれぞれ異なるサイズに変更するとしてもよい。これによって、境界線が移動させるだけで記憶領域及び非記憶領域のサイズを変更することができるので、そのための回路は小さくて済む。

32  
【0130】また、前記記憶領域サイズ変更回路は、前記記憶領域における論理アドレスと物理アドレスとの対応を示す記憶領域変換テーブルと、前記非記憶領域における論理アドレスと物理アドレスとの対応を示す非記憶領域変換テーブルと、前記電子機器からの命令に従って前記記憶領域変換テーブル及び前記非記憶領域変換テーブルを変更する変換テーブル変更部とを有し、前記記憶領域変換テーブル及び前記非記憶領域変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

33  
【0131】これによって、記憶領域と非記憶領域、変換テーブルが独立分離されているので、それぞれの領域サイズや論理アドレスと物理アドレスとの対応を個別に管理することが容易となる。また、前記記憶領域及び前記非記憶領域は、それぞれ、前記一定サイズの記憶領域を2分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非記憶領域変換テーブルは、論理アドレスの昇順で物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記記憶領域変換テーブルは、論理アドレスの昇順で物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられているとしてもよい。

34  
【0132】これによって、論理アドレスの昇順で使用していくことで、記憶領域と非記憶領域との境界付近の領域が使用される確立が低くなるので、その境界を移動させた場合に必要とされるデータ追跡や移動等の処理が容易となる。また、前記非記憶領域変換テーブルは、さらに、予めデータが格納された読み出し専用のメモリ回路を備えてもよい。これによって、他の半導体メモリカードと区別できる識別データ等を読み出し専用メモリに格納し、デジタル著作物をその識別データに依存させて格納したりすることで、著作権保護の機能が強化される。

35  
【0133】また、前記記憶領域及び前記非記憶領域は、前記電子機器によって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、前記記憶領域はさらに、前記電子機器が前記記憶領域にデータを書き込むためのアクセスする際に乱数を発生する乱数発生部を有し、前記記憶領域がアクセス制御部及び前記非記憶領域がアクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データ

36  
タに対応づけられた前記読み出し専用の記憶領域に書き込むとしてもよい。

37  
【0134】これによって、読み書き可能な記憶領域に対する不正な改ざん等が行われても、読み出し専用の記憶領域に格納された乱数との整合性を検査することで、そのような行為を検出することが可能となるので、より安全なデータ記録が実現される。また、前記制御回路は、さらに、前記記憶領域及び前記非記憶領域における論理アドレスと物理アドレスとの対応を示す変換テーブルを変更する変換テーブル変更部とを有し、前記記憶領域がアクセス制御部及び前記非記憶領域がアクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

38  
【0135】これによって、同一ファイルを作成する複数の記憶ブロックが断片化する現象が生じて、論理的に連続した記憶ブロックとなるように容易に変更することができ、同一ファイルへのアクセスが高速化される。また、前記制御回路はさらに、前記記憶領域及び前記非記憶領域に書き込むべきデータを暗号化するとともに、前記記憶領域及び前記非記憶領域から読み出されたデータを復号化する暗号化部を有してもよい。これによって、半導体メモリカードを接続して記憶領域及び非記憶領域のメモリ内容を確認読み出す等の不正な攻撃に耐えることが可能となる。

39  
【0136】また、前記非記憶領域は、フラッシュメモリであり、前記制御回路はさらに、前記電子機器からの命令に従って、前記記憶領域及び前記非記憶領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有してもよい。これによって、電子機器は、フラッシュメモリの書き換えに先立って、未消去の領域を知り、その領域を事前に消去しておくことができるので、高速な書き換えが可能となる。

40  
【0137】また、前記記憶領域は、記憶のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記記憶部による記憶に成功した電子機器を特定することができると識別情報を記憶しておくための識別情報記憶部と、前記記憶部から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否かを検査し、既に格納されている場合には、前記記憶部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有してもよい。

41  
【0138】これによって、半導体メモリカードと接続して使用する際にパスワードや超人データの入力が必要とされるという手間が回避されるので、不正に個人データが盗竊されて利用されるという不具合の発生が抑えられ

39  
【図5】同半導体メモリカードの外観及びハードウェア構成を示す図である。

40  
【図6】同半導体メモリカードの記憶領域の構成を示す図である。

41  
【図7】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

42  
【図8】音楽データ等のコンテンツを同半導体メモリカードに格納し、同半導体メモリカードに書き込み動作を示すフロー図である。

43  
【図9】音楽データ等のコンテンツを同半導体メモリカードから読み出し、同半導体メモリカードに書き込み動作を示すフロー図である。

44  
【図10】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

45  
【図11】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

46  
【図12】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

47  
【図13】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

48  
【図14】同半導体メモリカードの記憶領域の構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

49  
【図15】記憶のための同半導体メモリカードの構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

50  
【図16】記憶のための同半導体メモリカードの構成を示す図であり、(a)は各領域へのアクセスにおけるアドレスを示し、(b)は各領域のサイズの変更におけるアドレスを示し、(c)は同半導体メモリカードの領域を示す図である。

35

36

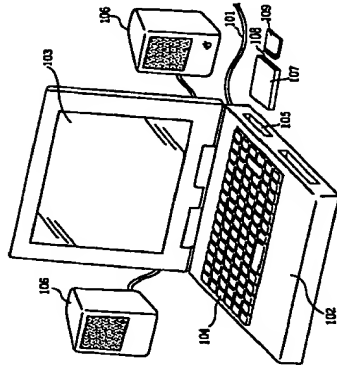
換テーブルを示し、(c)は認証領域専用の交換テーブルを示す。

【図19】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更後の状態を示す図であり、(a)はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、(b)は非認証領域専用の交換テーブルを示し、(c)は認証領域専用の交換テーブルを示す。

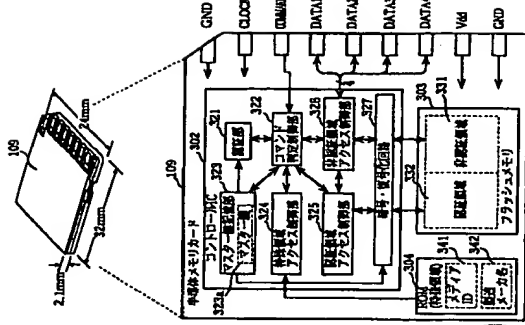
【符号の説明】

- 101 通信回路
- 102 PC
- 103 ディスプレイ
- 104 キーボード
- 105 メモリカードドライバ挿入口
- 106 スピーカ
- 107 メモリカードドライバ
- 108 メモリカード挿入口
- 109 メモリカード
- 110 CPU
- 111 ROM
- 112 RAM
- 113 通信ポート
- 114 内部バス
- 117 デスクランブラ
- 118 AACデコーダ
- 119 D/Aコンバータ
- 120 ハードディスク
- 201 プレーヤ
- 202 操作ボタン
- 203 液晶表示部
- 204 アナログ出力端子
- 205 デジタル出力端子
- 206 メモリカード挿入口
- 208 ヘッドフォン
- 210 CPU
- 211 ROM
- 212 RAM
- 213 通信ポート
- 214 内部バス
- 215 カード1/F部
- 216 認証回路
- 217 デスクランブラ
- 218 AACデコーダ
- 219 D/Aコンバータ
- 220 スピーカ
- 221 ディスプレイ
- 222 キーボード
- 223 メモリカードドライバ挿入口
- 224 スピーカ
- 302 コントローラIC
- 303 フラッシュメモリ
- 304 ROM (特殊領域)
- 10 321 認証部
- 322 コマンド判定制御部
- 323 マスター鍵記憶部
- 323a マスター鍵
- 323b 暗号化マスター鍵
- 324 特殊領域アクセス制御部
- 325 認証領域アクセス制御部
- 326 非認証領域アクセス制御部
- 327 暗号・復号化回路
- 331 非認証領域
- 20 332 認証領域
- 341 メディアID
- 342 製造メーカー名
- 343 セキュリティメディアID
- 425 暗号化キー
- 426 暗号化コンテンツ
- 427 ユーザーデータ
- 501 代替ブロック領域
- 812 読み出し回数
- 913 デジタル出力許可回数
- 30 1003 乱数発生器
- 1004 セクタ
- 1005 拡張領域
- 1006 ECCデータ
- 1007 時刻領域
- 1101 交換テーブル
- 1102 認証領域専用交換テーブル
- 1103 非認証領域専用交換テーブル
- 1203 未消去リスト
- 1301 マスター鍵
- 1302 機器固有ID
- 1310 機器固有ID暗号化領域
- 1311 ユーザーキー記憶領域

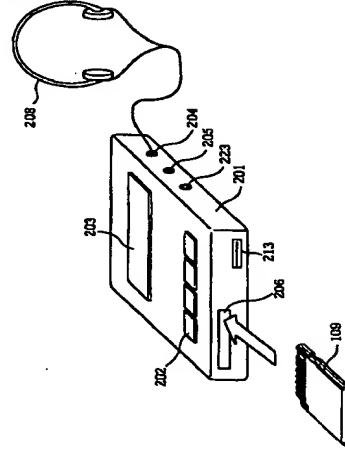
【図1】



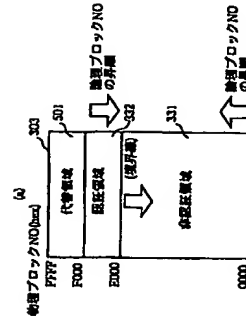
【図5】



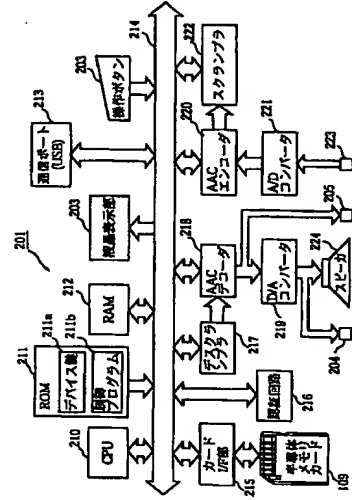
【図2】



【図18】



【図4】



(a)

| アドレス | 内容   |
|------|------|
| 0000 | 0000 |
| 0001 | 0001 |
| 0002 | 0002 |
| ...  | ...  |
| FFFF | FFFF |

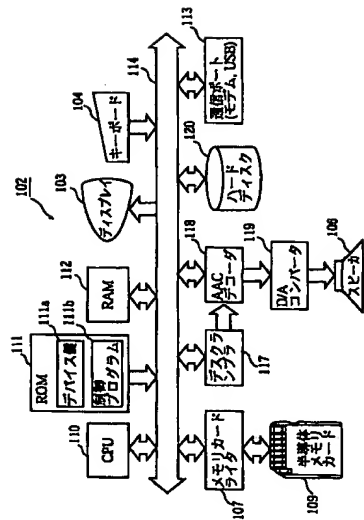
(b)

| アドレス | 内容   |
|------|------|
| 0000 | 0000 |
| 0001 | 0001 |
| 0002 | 0002 |
| ...  | ...  |
| FFFF | FFFF |

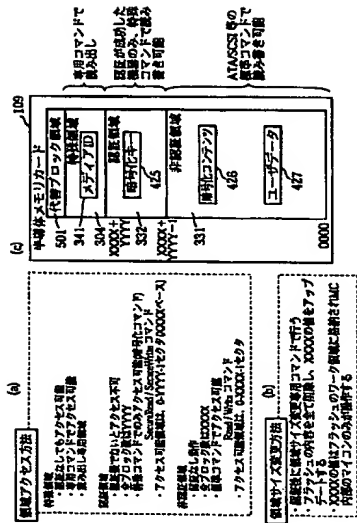
(c)

| アドレス | 内容   |
|------|------|
| 0000 | 0000 |
| 0001 | 0001 |
| 0002 | 0002 |
| ...  | ...  |
| FFFF | FFFF |

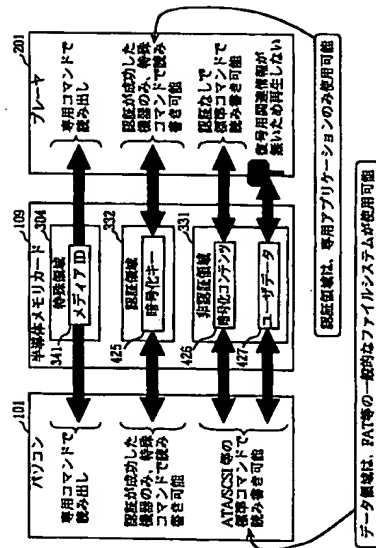
【図3】



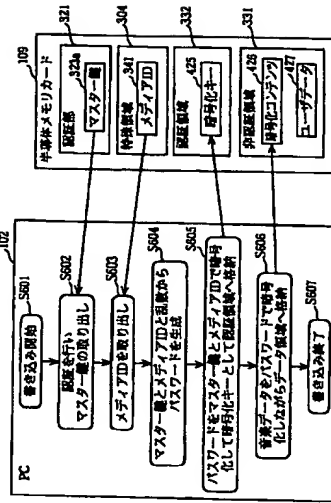
【図7】



【図6】

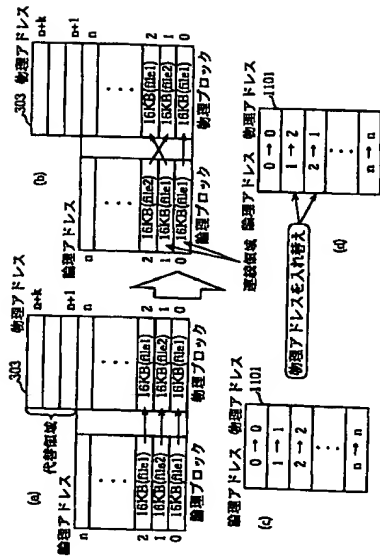


【図8】

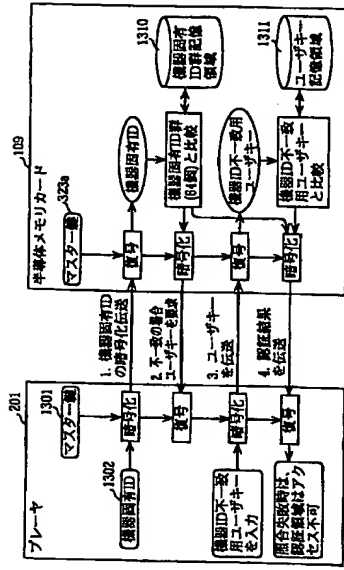




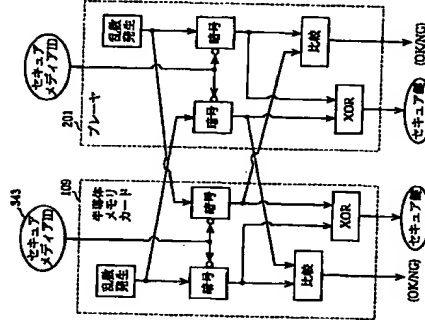
【図13】



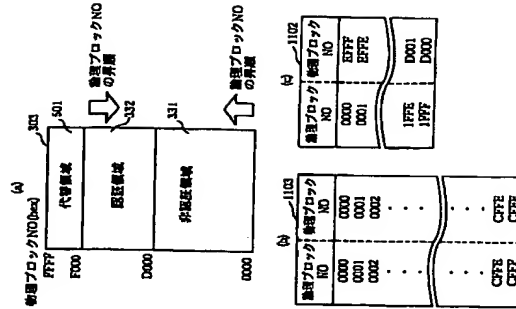
【図15】



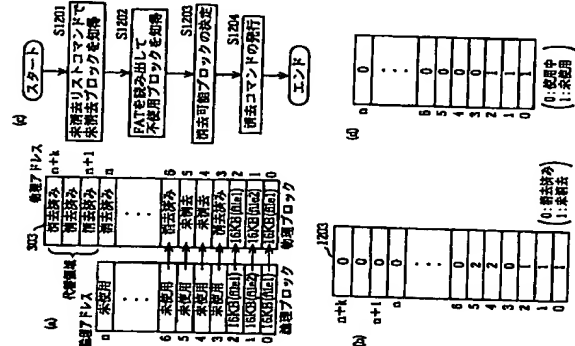
【図17】



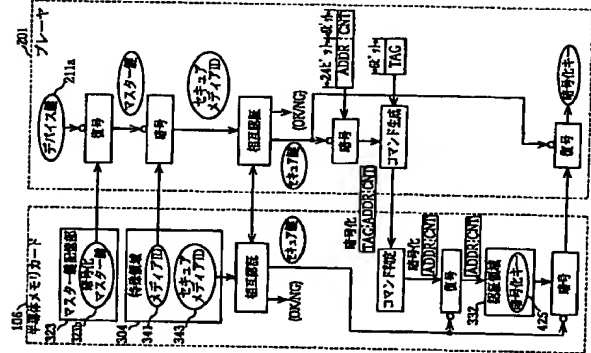
【図19】



【図14】



【図16】



フロントページの続き

- (72)発明者 小坂 雅之  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内
- (72)発明者 小坂 雅之  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内
- (72)発明者 小坂 雅之  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

時間 2001-14441

(27)

Fターム(参考) 5B017 A07 BA05 BA07 BB02 BB10  
CA14  
5B035 A06 A13 BB09 BC00 CA07  
CA11 CA38  
5B058 CA25 CA27 KA02 KA06 KA35  
YA16  
5J104 A07 KA02 NA02 NA05 NA33  
NA35 NA41 PA14